

United States District Court

NORTHERN

DISTRICT OF

NOV 18 2009

CLERK, U.S. DISTRICT COURT
By TEXAS Deputy

In the Matter of the Search of

(Name, address or Brief description of person, property or premises to be searched)

1623 Main Street, Apt. 804
Dallas, Texas 75201

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

CASE NUMBER: 3:09-MJ-403

I Karla R. Brainard being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation (FBI) and have reason to believe that XX
on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

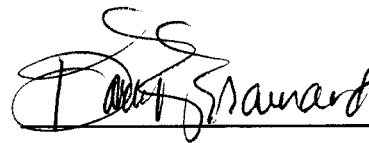
in the NORTHERN District of TEXAS there is now
concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed,
concerning a violation of Title 18 United States Code, Section(s) 2252 and 2252A. The facts to
support a finding of Probable Cause are as follows:

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT KARLA R. BRAINARD).

Continued on the attached sheet and made a part hereof. XX Yes No



Signature of Affiant
KARLA R. BRAINARD
Special Agent, FBI

Sworn to before me, and subscribed in my presence

November 18, 2009

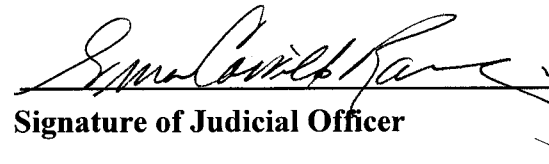
Date

IRMA C. RAMIREZ
United States Magistrate Judge

Name and Title of Judicial Officer

at Dallas, Texas

City and State



Signature of Judicial Officer

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The premises to be searched is **1623 Main Street, Apt. 804, Dallas Texas 75201** (the "SUBJECT PREMISES"). The SUBJECT PREMISES is more particularly described as the historic "Wilson Building" a 12-story apartment building. The premises is located on the south west corner of the intersection of Evary and Main Street in downtown Dallas, Texas. The building front office door is located on Main Street and faces East. Apartment 804 is located on the 8th floor on the south side of the building. The apartment door is brown with a large brass-style door knob. Directly adjacent to the front door are the numbers 804 on a brass and black plate. Apartment 804 is located beside the black service elevators to the parking garage. The SUBJECT PREMISES is located in Dallas County which is within the Northern District of Texas.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of [target's e-mail address] by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache

- information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
 9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
 10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
 11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs

and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.
13. Any and all visual depictions of minors.
14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
15. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or

lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

16. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
17. Credit card information, including, but not limited to, bills and payment records.
18. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.
19. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Karla R. Brainard being duly sworn, depose and state the following:

1. I am a special agent with the Federal Bureau of Investigation (FBI), assigned to the Dallas Division of the Federal Bureau of Investigation, Dallas, Texas. I have been so employed since August 06, 1995. I have a Bachelor degree in Criminal Justice from Texas State University, San Marcos, Texas. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C §§ 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have participated in investigations of these violations. In the course of these investigations, I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, many of which have involved child exploitation and/or child pornography offenses.

2. This affidavit is submitted in support of an application for a search warrant for the residence of MONTE ALBERT MELUGIN, **1623 Main Street, Apartment 804 Dallas, Texas 75201, located in Dallas County, within the Northern District of Texas** (hereinafter known as the "Subject Premises"), and the computer(s) located therein, for evidence of violations of Title 18, United States Code, Sections 2252 and 2252A. The Subject Premises is more fully described in Attachment A hereto. The items to be

searched for and seized are described more particularly in Attachment B hereto.

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A are presently located at the Subject Premises.

RELEVANT STATUTES

4. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

5. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

7. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual

depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

9. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

10. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

11. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

12. “Internet Service Providers” or “ISPs” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail,

remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

13. “Domain Name” refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely

identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

14. “Log Files” are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

15. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

16. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

17. “Uniform Resource Locator” or “Universal Resource Locator” or “URL” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a

domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

18. The terms “records”, “documents”, and “materials”, as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

19. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others), can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or (normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

21 Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251-2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

22. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used).

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;
- b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas

exist that are likely to appear in the evidence described in Attachment B;
and

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND REGARDING THE INTERNET

23. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet extensively since 2000. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

24. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at

the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

25. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

26. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

27. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

28. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for

years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

P2P FILE-SHARING IS A GROWING PHENOMENON

29. A growing phenomenon on the Internet is the peer-to-peer file sharing program (P2P). The P2P file-sharing allows individuals to meet each other through the Internet, engage in social networking, and trade files.

30. The latest evolution of P2P software is a program that allows a user to set up his own private P2P network contacts. File-sharing through this new and publicly

available P2P file sharing program is limited only to other users who have been added to a private list of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the listed files that the other user has made available to download, selected desired files from the list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer file containing the file.

31. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

32. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address identifies the location of the computer with which the address is associated, make it possible for data to be transferred between computers.

33. Third-party software is also available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet an local network traffic.

BACKGROUND OF INVESTIGATION

34. On May 26, 2009, Special Agent (SA) Alexis Carpinteri, Miami Division, using a computer connected to the Internet, launched a publicly available P2P file sharing program from an Innocent Images Unit of the FBI, located in Miami, Florida. SA

Carpinteri queried a network of friends and observed an individual using the username "SKITTLES16" was logged onto the network allowing SA Carpinteri to view and download files from "SKITTLES16" computer that SKITTLES16 selected to share with other users.

35. SA Carpinteri browsed SKITTLES16's shared folders and observed approximately 1250 images and video files depicting child pornography. SA Carpinteri selected eighteen (18) images and video files of child pornography and began to download these files directly from SKITTLES16's computer. SA Carpinteri was able to determine that the IP address for SKITTLES16's computer was 70.116.134.157.

36. When reviewed, all or most of the eighteen (18) image and video files depicted child pornography. Five (5) files downloaded that depicted child pornography had the following names and are described briefly:

- a. **Aaron(35).jpg** This image file depicts a blonde prepubescent child with his hands on a erect adult male penis. The penis is inserted into the mouth of the prepubescent child.
- b) **Aaron(286).jpg** This image file depicts a minor male with an erect male penis in his mouth. An adult male's left hand is holding the back of the prepubescent child's head.
- c) **Aaron (290).jpg** This image file depicts an erect adult male penis penetrating a prepubescent male's anus. The right hand of the adult male is inserting the penis into the anus of the minor male child.
- d) **Aaron(278).jpg** This image file depicts an adult male penis fully inserted into the anus of a prepubescent male. The prepubescent male is laying on his back and his hands/arms are at his sides.

- e) **Aaron Fabi(36).jpg** This image file depicts two nude prepubescent males. One of the prepubescent males is performing oral sex (the penis of one male is in the mouth of the other male) on the other prepubescent male.

37. SA Carpinteri used the program Commview in order to identify the Internet Protocol (IP) address utilized by "Skittles16." It was determine to be 70.116.134.157.

38. SA Carpinteri searched a publicly available database and the IP address 70.116.134.157 which resolved back to Road Runner - Time Warner Cable.

39. An administrative subpoena served on Road Runner-Time Warner Cable revealed that IP address 70.116.134.157 was assigned to the account of MONTE MELUGIN, 1623 Main Street, Apartment 804, Dallas, TX 75201 and using e-mail address: mmelugin@tx.rr.com.

40. Road Runner-Time Warner cable subscriber information on MONTE MELUGIN revealed that MONTE MELUGIN's internet service to 1623 Main Street, #804 was initiated on 10/18/2008.

41. Road Runner-Time Warner Cable provided the contact number of (940)231-9938 for MONTE MELUGIN.

42. A search of a public data base revealed that 1623 Main Street, Dallas, TX is known as "The Wilson Building." The Wilson Building is managed by Forest City Residential in The Mercantile Place.

43. A Federal Grand Jury Subpoena served on The Mercantile Place, Forest City Residential revealed that MONTE A. MELUGIN moved into 1623 Main Street, Apartment 804, Dallas, TX on 10/14/2008.

44. According to the leasing records, MONTE A. MELUGIN continues to reside at 1623 Main Street, Apartment 804, Dallas, TX.

45. According to the leasing records, MONTE A. MELUGIN provided a contact number as (940)231-9938 and an e-mail address of mmelugin@tx.rr.com.

**CHARACTERISTICS COMMON TO INDIVIDUALS IN THE
DISTRIBUTION, TRANSPORTATION, RECEIPT, OR POSSESSION AND
ATTEMPTED DISTRIBUTION, TRANSPORTATION, RECEIPT, OR
POSSESSION OF CHILD PORNOGRAPHY**

46. As set forth above, probable cause exists to believe that an individual at 1623 Main Street, Apt. 804, Dallas, TX has distributed, transport, receive or possessed child pornography, or has attempted to commit these crimes.

47. Based on my previous investigative experience related to child pornography investigations, including investigations of subjects who possess, trade, distribute, produce or receive child pornography, subscribed to websites offering access to child pornography, and engage in conversations related to the sexual exploitation of children, I have learned that individuals who subscribed to such websites are often individuals who have a sexual interest in children and in images of children, and who download images and videos of child pornography. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt, distribution and/or possession of child pornography:

- a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who have a sexual interest in children or images of children often maintain the images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These files, also referred to as "collections" are often maintained for several years and are kept close by, usually at the residence, to enable the individual to view the images, which are valued highly.
- e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often

maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

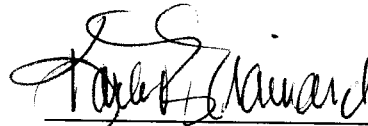
- f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

48. Based on the information I have at this time, MELUGIN fits the profile of an individual who collects child pornography and therefore is likely to maintain, and even increase, his collection. At the time of the download by SA Carpinteri, MELUGIN's sharing folder contained approximately 1250 files containing child pornography and/or contained descriptive information of its contents in its naming convention with filenames consistent with child pornography. SA Carpinteri was able to preview most of the files prior to downloading them and determined they were child pornography files. The very nature of the P2P software program is to share files in an attempt to increase a user's collection of files. The software is only successful if the users are sharing their collections, so that each user can obtain copies of images and make available their images, to that all users benefit and increase their collection of images. Given the size of MELUGIN's collection that was available for trade, and use of software that encourages trading and maintaining large collections of images, I believe MELUGIN is a collector of child pornography and further, that a search of his premises will reveal evidence of this collection.

CONCLUSION

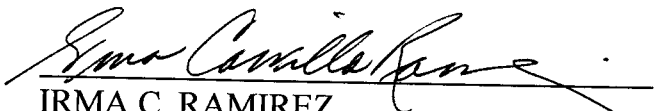
49. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. §§ 2252 and 2252A. This probable cause is based in part on the email transactions of images of child pornography that were sent to the residence at 1623 Main Street, Apt. 804, Dallas, Texas.

50. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.



Karla R. Brainard, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 18th day of November, 2009



IRMA C. RAMIREZ
UNITED STATES MAGISTRATE JUDGE